



4

04co 09-13-01

PATENT
3587-0106P

THE U.S. PATENT AND TRADEMARK OFFICE

Applicant: Kaleedhass KARTHIK Conf.:
Appl. No.: 09/893,714 Group:
Filed: June 29, 2001 Examiner:
For: BIOMETRIC VERIFICATION FOR ELECTRONIC
TRANSACTIONS OVER THE WEB

#f

L E T T E R

Assistant Commissioner for Patents September 25, 2001
Washington, DC 20231

Sir:

Under the provisions of 35 U.S.C. § 119 and 37 C.F.R. § 1.55(a), the applicant(s) hereby claim(s) the right of priority based on the following application(s):

<u>Country</u>	<u>Application No.</u>	<u>Filed</u>
MALAYSIA	PI 2000 2960	June 29, 2000

A certified copy of the above-noted application(s) is(are) attached hereto.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fee required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Respectfully submitted,

BIRCH, STEWART, KOLASCH & BIRCH, LLP

By Paul C. Slattery
James M. Slattery, #28,380
P.O. Box 747 #43,368
Falls Church, VA 22040-0747
(703) 205-8000

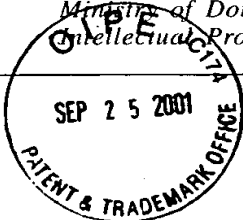
JMS/PCL/cl
3587-0106P

Attachment



KEMENTERIAN PERDAGANGAN DALAM NEGERI
DAN HAL-EHWAL PENGGUNA MALAYSIA,
BAHAGIAN HARTA INTELEK,
TINGKAT 27, 30 DAN 32,
MENARA DAYABUMI,
JALAN SULTAN HISHAMUDDIN,
50623 KUALA LUMPUR

Ministry of Domestic Trade and Consumer Affairs Malaysia,
Intellectual Property Division



3587-0106P
filed 6-29-01
09/893,714
Kaleedhass KARTHIK
BSKB, LLP
(703) 205-8000
181
Telefon: 03-2741000
Fax: 2741332

Fail Tuan:

Fail Kita:

Tarikh:

#4

To:

P. KANDIAH

KANDIAH & ASSOCIATES SDN. BHD.
Suite 8 - 7 - 2, Menara Mutiara Bangsar
Jalan Liku, Off. Jalan Bangsar,
59100 Kuala Lumpur
MALAYSIA

PATENT APPLICATION NO: PI 2000 2960

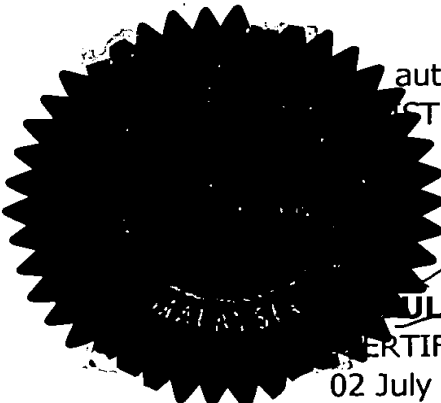
This is to certify that annexed hereto is a true copy from the records of the Registry of Trade Marks and Patents, Malaysia of the application as originally filed which is identified therein.

authority of the
REGISTRAR OF PATENTS


ABDUL RAHMAN RAMLI

(CERTIFYING OFFICER)

02 July 2001





KEMENTERIAN PERDAGANGAN DALAM NEGERI
DAN HAL EHWAL PENGGUNA MALAYSIA
BAHAGIAN HARTA INTELEK,
TINGKAT 27 & 32,
MENARA DAYABUMI,
JALAN SULTAN HISHAMUDDIN,
50623 KUALA LUMPUR.
Ministry of Domestic Trade and Consumer Affairs Malaysia
Intellectual Property Division.


Telefon : 03-22742100
Fax : 03-22741332

CERTIFICATE OF FILING

APPLICANT : MULTIMEDIA GLORY SDN. BHD.
APPLICATION NO. : PI 20002960
REQUEST RECEIVED ON : 29/06/2000
FILING DATE : 29/06/2000
AGENT'S/APPLICANT'S : PK/P704/MG/2000
FILE REF.

Please find attached, a copy of the Request Form relating to the above application, with the filing date and application number marked thereon in accordance with Regulation 25(1).

Date : 03/07/2000


.....
(Hasnon Bt. Alang Mohd Rashid)
for Registrar of Patents

To : P. KANDIAH,
C/O KANDIAH & ASSOCIATES SDN BHD,
SUITE 8-7-2, MENARA MUTIARA BANGSAR,
JALAN LIKU, OFF JALAN BANGSAR,
59100 KUALA LUMPUR,
MALAYSIA.

Patents Form No. 1
PATENTS ACT 1983

REQUEST FOR GRANT OF PATENT
(Regulation 7(1))

To: The Registrar of Patents
Patent Registration Office
Kuala Lumpur
Malaysia

For Official Use

APPLICATION RECEIVED ON: 01/06/2000

Fee received on: 01/06/2000

Amount: RM 200.00

*Cheque / Postal Order / Money Order / Draft /
Cash No.: 505293

Please submit this Form in duplicate together
with the prescribed fee.

Applicant's file reference: **PK/P704/MG/2000**

**I. THE APPLICANT(S) REQUEST(S) THE GRANT OF A PATENT IN RESPECT OF THE
FOLLOWING PARTICULARS:**

**TITLE OF INVENTION: BIOMETRIC VERIFICATION FOR ELECTRONIC
TRANSACTIONS OVER THE WEB**

**II. APPLICANT(S) (the data concerning each applicant must appear in this box or, if the space is
sufficient, in the space below)**

Name: MULTIMEDIA GLORY SDN. BHD.

I.C./Passport No:

**Address: 57 M, Jalan Thamba Pillai
Brickfields, 50470 Kuala Lumpur
Malaysia**

**Address for service in Malaysia: Suite 8-7-2
Menara Mutiara Bangsar
Jalan Riong, Bangsar
59100 Kuala Lumpur
Tel: 284 7872 Fax: 284 1125**

**Nationality: A Company Established Under the Laws of
Malaysia.**

- Permanent residence or principal place of business:

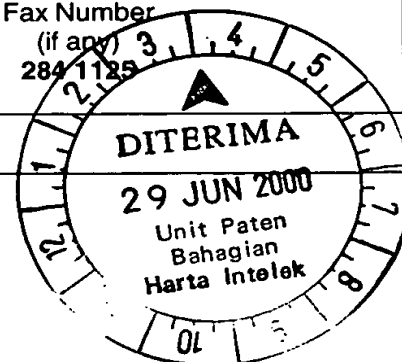
AS ABOVE

**Telephone Number
(if any)
284 7872**

**Fax Number
(if any)
284 1125**

Additional Information (if any)

20002960



III. INVENTOR

Applicant is the inventor:

Yes ☐

No ☒

If the applicant is not the inventor:

Name of the inventors: **Karthik Kaleedhass S/O V.S. Kalidas**
Passport No : A 3636265 (Indian Passsport)

Address of inventors: **C-1705 Palm Court**
Brickfields
50470 Kuala Lumpur
(A Citizen of India)

A statement justifying the applicant's right to the patent accompanies this Form:

Yes ☒

No ☐

Additional Information (if any)

IV. AGENT OR REPRESENTATIVE:

Applicant has appointed a patent agent in accompanying Form No. 17

Yes ☒

No ☐

Agent's Registration No: **PA 90/019**

Applicants have appointed **P. Kandiah** to be their common representative

IV. DIVISIONAL APPLICATION

This application is a divisional application

Yes ☐

No ☐

The benefit of the

Filing date

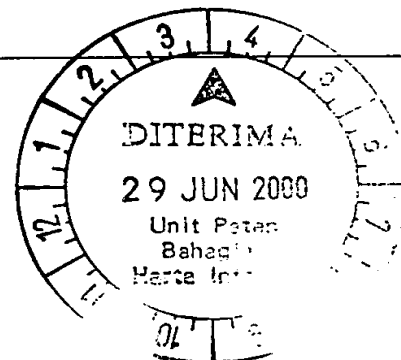
Priority date

Of the initial application is claimed in as much as the subject matter of the present application is contained in the initial application identified below: -

Initial Application No:

Date of filing of initial application:

20002960



VI. DISCLOSURES TO BE DISREGARDED FOR PRIOR ART PURPOSES

Additional information is contained in supplemental box:

- (a) Disclosure was due to acts of applicant or his predecessor in title

Date of disclosure:

- (b) Disclosure was due to abuse of rights of applicant or his predecessor in title

Date of disclosure:

A statement specifying in more detail the facts concerning the disclosure accompanies this Form

Yes ☐

No ☐

Additional Information (if any)

VII. PRIORITY CLAIM (if any)

The priority of an earlier application is claimed as follows:

Country (if the earlier application is a regional or international application, indicate the office with which it is filed):

Filing Date:

Application No:

Symbol of the International Patent Classification:

If not yet allocated, please tick

☐

The priority of more than one earlier application is claimed:

Yes ☐

No ☐

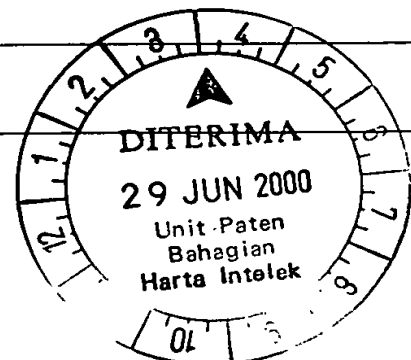
The certified copy of the earlier application(s) accompanies this Form:

Yes ☐

No ☐

If No, it will be furnished by (if requested by Registrar)

Additional Information (if any) :



20002333

VIII. CHECK LIST

A. This application contains the following:

1.	Request	1	Sheets
2.	Description	32	Sheets
3.	Claim	1	Sheets
4.	Abstract	1	Sheets
5.	Drawing	13	Sheets
	Total	48	Sheets

B. This Form, as filed, is accompanied by the items checked below:

(a)	signed Form No. 17	<input checked="" type="checkbox"/>
(b)	declaration that inventor does not wish to be named in the patent	<input type="checkbox"/>
(c)	statement justifying applicant's right to the patent	<input checked="" type="checkbox"/>
(d)	statement that certain disclosures be disregarded (to follow)	<input type="checkbox"/>
(e)	priority document (certified copy of earlier application)	<input type="checkbox"/>
(f)	cash, cheque, money order, banker's draft or postal order for the payment of application fee	<input checked="" type="checkbox"/>
(g)	other documents (specify) -	<input type="checkbox"/>

XI. SIGNATURE:

P. Kandiah

P. Kandiah
 ** (Applicant/Agent)

29th June 2000
 (Date)

If Agent, indicates Agent's Registration No: **PA 90/019**

For Official Use

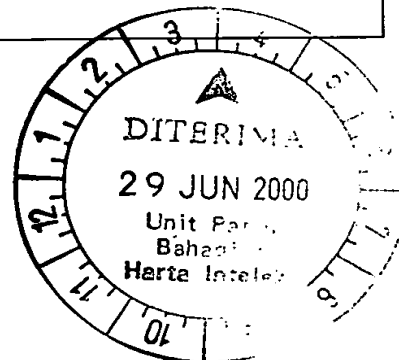
3. Date application received:

4. Date of receipt of correction, later filed papers or drawings completing the application:

* Delete whichever does not apply.

** Type name under signature and delete whichever does not apply.

20002960



STATEMENT JUSTIFYING APPLICANT'S RIGHT TO PATENT
Regulation 10(2), Patents Regulations 1986
Patents Act, 1983

- i. Agent's File Ref : **PK/P704/MG/2000**
- ii. Application No:
- iii. Applicant : **Multimedia Glory Sdn. Bhd.**
57M, Jalan Thamba Pillai
Brickfields, 50470 Kuala Lumpur
Malaysia

iv. Title of Invention: **BIOMETRIC VERIFICATION FOR ELECTRONIC TRANSACTIONS OVER THE WEB**

v. Pursuant to Regulation 10(2) of the Patents Regulations 1986 I believe that the inventor(s) of the above stated application is/are as follows: -

Name of the inventor(s) :

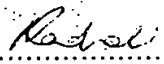
KARTHIK KALEEDHASS S/O V.S.KALIDAS
C-1705 Palm Court, Brickfields
50470 Kuala Lumpur
Passport No : A3636265 (Indian Passport)

(A Citizen of India)

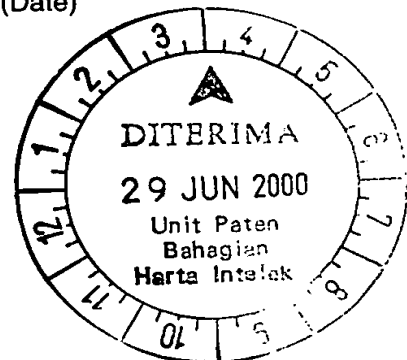
vi. Applicant's right to the invention:

The Applicant's Right to the Invention is by virtue of Contract of Employment from the Inventor .

vii. Signature:


P. Kandiah
Reg # PA 90/019

29/6/2000
(Date)



20002960

BIOMETRIC VERIFICATION FOR ELECTRONIC TRANSACTIONS OVER THE WEB

FIELD OF INVENTION

5 This invention relates to security systems for **electronic commerce**, and more particularly to a method for minimizing the potential for unauthorized use of digital information, particularly software programs, digital content and other computer information. This invention can also be used in other processes which requires authentication of the users.

BACKGROUND OF THE INVENTION

10 **Electronic commerce**, or e-commerce as it is commonly called, includes the transfer of orders or other sales communications, credit information, electronic "funds", and digital products. **Electronic commerce** has been recognized as offering the promise of providing speed and convenience to many types of commercial activities. Interest in **electronic commerce** has heightened with the advent of widely accessible communication systems such
15 as the Internet. Other means for providing **electronic commerce** include direct telephone line connections, interactive cable or television services, telefacsimile services, local and wide area network communications and the like. Electronic data communication technologies, particularly
the Internet, have greatly enhanced marketing and retail opportunities and activities.

To a large extent, the promise of **electronic commerce** has not been fully realized,
20 partially because of concerns with security such as the potential for unauthorized manipulation of information. Such unauthorized manipulation of information includes diverting electronic fund transfers and delivery of unauthorized softwares (also referred to as "bootleg" or "pirated" software) to unauthorized destinations.

The electronic commerce operations especially electronic commerce transactions requires
25 security as it is based over an open network. The present security solutions includes encryption, that is normally undertaken to ensure privacy so that no person(s) other than the intended recipient can decrypt the information but it does not guarantee the authenticity of the person who initiates the transaction.

"Internet Banking" is a technology advancement that provides a convenient way of
30 banking at home or from any other place by using a computer. As the word "Internet", the internet banking is over an open network and the security for authentication must be in place to

secure the transactions. As all the security solutions were in place, what could be possibly wrong with the current system of security in Internet Banking?

For example, credit card transactions over the internet is a way of online payment and is a part of Internet banking. Credit cards were used in internet, mainly for buying products, services online and for other authentication purposes. The current way of using the credit card is, by providing the credit card number, expiry date or Postal Code and other information required for credit card payments. All these information are used to verify the validity of the card and the available balance. But there is no system to check the identity and authenticity of the person using the credit card in online transactions.

The identity of the person initiating the credit card transaction is required as the credit card can be used by providing the Credit Card number and the expiry date or any other information required. Even a child can buy products or services online using the credit card by entering the Credit Card number and other required information without the knowledge of the card holder, if this information is known.

This can be done with or without an intention, but the security lapse is exploited. Due to this, the wrong person would be charged for the transaction resulting in financial losses. These losses that occur due to the failure in authentication, can be removed if the invented security solution is implemented.

The security solution can also be implemented in an Automated Teller Machines where the security lapse in authentication, is evident. As per the recent market study, it is observed that, considerable sum of money per day per ATM is lost through these fraudulent transactions. The reason being the insufficient security features to authenticate the customer in the ATM, the person starts with the transactions when he or she inserts the card and the PIN. Even an onlooker can transact with the information.

The security solution can also be used to authenticate the persons refilling the cash in the ATM.

A person issuing a cheque must authenticate the cheque when the cheque is presented for clearance depending upon the permissible limit and the value of the cheque. At present the universal method for this authentication is a confirmation from the cheque issuer by telephone and an authentication of the person who confirmed is not guaranteed.

Patient history is an essential requirement to treat patients during emergencies like critical illness and accidents. With advent of technology patient history can be stored online

using internet, so that the patient or the doctor can have easy access to the information. In this case the security (authentication) should be adequate to ensure that the information does not get into wrong hands.

The invention can also be used to screen blood donors for critical illness and other blood transmitted diseases.

The security solution can be extended to provide security at Automated Teller Machines, Access Control systems, Online Banking, Banking Services, Medical portals, e-business, networking, inter-networking, cellular phone, data ports, printer, fax machine, notebook computers, palm top computers, palm pilot, microfiche devices, scanner, cameras, modems, communication access, personal data systems, pagers, vending machines, PC terminals, information kiosks, Point of Sales (POS), sharing valuable information with authorized users, wireless transmission, telecommunications, telephony, smartCard access controls, remote access networks, debit cards, credit cards, prepaid cards, magnetic cards, phone cards, identifying devices, hotel room key cards, net PC, phone having access to internet, data security, bank locker systems, interbank transactions.

The security solution according to the present invention can be used to replace passwords which are hard to remember, Unauthorized persons can gain access to resources if they come to know of the password. The security solution ensures that only authorized persons are given access to the secured resources.

SUMMARY OF THE INVENTION

The invention disclosed herein uses "biometrics" technology, that is verification/identification of an individual's unique physical or behavioral traits. Types of "biometrics" methods include fingerprint scanning, iris scanning, retina scanning, handwriting analysis, handprint recognition and voice recognition. The invention may also use the combination of all or some "biometrics" technology.

The invention disclosed herein utilizes "biometrics" technology for authentication to permit world wide electronic commercial transactions to be carried out in a highly secured manner over an open network.

A security system for electronic commerce to verify the authenticity of a user comprising; installation of a server authentication program in a web-server at a website of a web-service provider; downloading and installation of client software component at a

workstation of the client; integration of the server authentication program with existing web-application with the web-service provider; user entering the existing security parameters; activation of biometrics scanner pre-installed at workstation of client gathering biometrics image from biometric scanner, identifying characteristics of biometrics image and converting into digital data; compression and encryption of data from biometric scanner; transmittance of compressed and encrypted data to web-server; comparison of encrypted data with data stored in database; sending of status codes of comparison, if comparison is successful, to application at web-service provider.

The invention also implements compression and encryption to protect the "biometrics" identification data.

The invention does not store the image of the "biometrics" information, instead stores the data on the unique physical or behavioral traits.

The invention includes a server authentication program which verifies the scanned "biometrics" information with the information stored in the database.

The invention includes a server containing the authentication program which may be connected to an open network or to a local network.

The invention provides flexibility in installing the server authentication program in other servers which is not part of invention.

The invention also provides flexibility to install the authentication program for a website.

The invention also provides functionality to implement the authentication module for verification of the "biometrics" information in embedded systems.

The invention uses the Database Servers like Relation DataBase Management System (RDBMS), DataBase Management System and other data storage system for storing the "biometrics" information.

The invention stores the "Biometrics" information based on the unique identification of the user in the real world, in the internet or the uniquely generated information in the Database Servers.

The invention includes a compatible "biometrics" scanner or reader to gather the "biometrics" information of an individual.

The invention includes the client component that consists of hardware drivers, "biometrics" retrieval program which needs to be installed in the computer to gather the "biometrics" information from the connected "biometrics" scanner.

5 In the invention the program in the server and in the client may be connected over an open or private network or a secured open or private network.

The invention disclosed herein permits ordering of goods and services in a secured manner.

The invention disclosed herein also permits the payment for goods and services only from the authorized sources.

10 The invention disclosed herein also helps in checking the person's identity in a transaction.

The invention disclosed herein permits access to the resources to only authorized persons.

15 The invention disclosed herein facilitates online enrollment of new or existing user's fingerprint.

The invention disclosed herein allows to store additional fingerprint for an existing user.

The invention disclosed herein provides online verification test for the enrollment of fingerprints.

20 The invention disclosed herein allows more than one fingerprint of the same person to be stored. The users can even store the fingerprint of all the fingers for easy authentication.

The invention disclosed herein ensures that only the authorized persons get the required information from the secured sources.

The invention also permits the handling of various stock transactions, including tenders, in a secured manner over an open network.

25 The invention disclosed herein can be used for electronic commerce transaction for verifying the authenticity of the transaction by the authorized person.

The invention disclosed herein enables all web-sites to use "biometrics" verification technology as part of their authentication process.

30 The invention disclosed herein also permits the authorized payment or transfers of electronic cash over an open network.

One principal advantage of the invention is the ability to utilize "biometrics" technology to undertake secured financial and other electronic transactions over a publicly accessible networks

5 Advantage of the invention resides in automatic and controlled access to network applications utilizing "biometrics" technology.

Advantage of the invention resides in the creation and processing of electronic cash with the highest degree of convenience as currency and with the same degree of security.

Advantage of the invention resides in reducing the credit card frauds, frauds at Automated Teller Machines.

10 Advantage of the invention resides in any web-site that can instantly be linked to the "biometrics" authentication service which is a part of the invention, without major changes in the existing applications at the web-site.

Advantage of the invention is in the integration of "biometrics" technology with the existing available authentication methods to facilitate secure electronic transactions over an unsecured network.

15 Advantage of the invention is that, during authentication, the fingerprint verification is done with all the fingerprints stored in the database, as such there is no necessity for the users to remember the finger to be placed on the sensor for verification.

Other advantages and objects of the invention are achieved by integrating the invention with the existing web-sites by linking the existing authentication methods or by embedding the invention into the existing authentication methods terms providing the highest level of security during authentication.

20 The invention is also directed to a method of conducting electronic - commerce transactions over an unsecured network by registering a biometric parameter such as fingerprint of a user and authenticating electronic transactions using a "biometrics" verification technology. In this way, each and every transaction in the internet can be secured. This method has been applied to a number of business transactions such as in authenticating offers, counteroffers and acceptance in a contract negotiations process; authenticating offers, bids and/or confirmations of sale in an auction process; authenticating a guarantee; authenticating orders and/or payments in a purchase/sale transaction; authenticating transfers of intangible personal property; authenticating tender offers and/or one or more tenders of shares of stock;

authenticating certificates of insurance; authenticating transfers of intangibles related to an escrow transaction and authenticating transfers of electronic money.

Another object and advantage of the present is that the invention will become readily apparent to those skilled in the art from the following detailed description, wherein only the preferred embodiment of the invention is shown and described, simply by way of illustration of the best mode contemplated of carrying out the invention. As will be realized, the invention is capable of other different embodiments, and some of its details are capable of modifications in various obvious fields, all without departing from the invention. Accordingly, the drawing and description are to be regarded as illustrative in nature, but not as a restrictive.

The invention disclosed herein can be used to screen blood donors for critical illnesses and other blood transmitted diseases.

BRIEF DESCRIPTION OF DRAWINGS

Figure 1, is a flow diagram of the process for online enrollment of "biometrics" data for new users in a web-site.

Figure 2, is a flow diagram of the process for online enrollment of "biometrics" data for an existing user in a web-site.

Figure 3, is a flow diagram of the process for online enrollment additional "biometrics" data for an existing enrolled user in a web-site.

Figure 4, is a flow diagram of the process for online verification of stored "biometrics" data for an existing enrolled user in a web-site.

Figure 5, is a flow diagram of the process for online enrollment of "biometrics" data for Credit Card users.

Figure 6, is a flow diagram of the process for online authentication using biometrics in an electronic commerce transaction for credit card users.

Figure 7, is a flow diagram of the process for online authentication using biometrics in an electronic commerce transaction for other identification methods.

Figure 8, is a flow diagram of the process for online authentication using biometrics in an ATM transaction.

Figure 9, is a flow diagram of the process for online authentication using biometrics and using invention's authentication server.

Figure 10, is a flow diagram of the process for online authentication using biometrics in an internet banking transaction.

Figure 11, is a flow diagram of the process for online authentication in software applications.

5

DETAILED DESCRIPTION OF THE INVENTION

Figure 1, is a flow diagram of a process for online enrollment of "biometrics" data for a new users in a web-site. The process explained in the diagram is for storing the "biometrics" data, that will be used for verification during an authentication on a web-site. The enrollment process is a standard process but it vary depending upon the requirements of the web-site. The "biometrics" data will be stored in the database server for an user identified by the unique identity in the web-site or in the real world. The database server will reside along with the web-site so as to maintain the consistency of the data for other web-sites stored on the same server.

15 The process initiator is the client software component which is installed and used in the step 102. Before the step 102, the user enters the required information to create a temporary/permanent unique identification in the Web-Site as in step 101. The information required by the web-site is designed and implemented in the web-site by an administrator of the web-site. The web-site will call the invention's authentication program for activating the core process of enrollment.

20 The basic requirement for the invention to select the "biometrics" data, is an unique identifier, also used during verification/authentication. This unique identifier that is generated by the web-site or entered by the user will be sent to the invention's authentication module. The authentication module will then redirect the web-browser to the enrollment page and the step 25 102 start to process the data given.

The identifier is unique throughout the user database of the invention's database server. The client components introduced in step 102 of this process, will be in the form of a downloadable components (like ActiveX, Plug-in, Java Applets), compatible with all available web-browsers, which is the main user-interface for the user. The versions of the component will be maintained so that the Web-Browser will automatically download the latest components.

30

The execution of the step 102, is wholly taken care of by the browser and the deployment of the components is made compatible for the same. In step 102, all the drivers and other necessary software components will be downloaded to the client PC.

5 At step 103, the client component will start processing the data. Firstly, it will check for the existing "Biometrics" scanner. This is done by communicating, with the "Biometrics" scanner specified protocol, and the "Biometrics" Scanner drivers supplied by the vendor.

10 In case the "Biometrics" scanner is not present or connected and if there is any problem in communicating with the "Biometrics" scanner by the client component, the client component will immediately display a message (step 104) informing the cause related to the communication problem.

The client component will also guide the user with the troubleshooting steps (if any) to rectify the communication problem. If the problem persists, the client component will immediately terminate the process by disconnecting itself from the server component. When the server component is disconnected from the client component, it will terminate the process at the server and will redirect the web-browser to the web-page, from where the user will be guided.

15 However, if the "Biometrics" scanner is present and connected (step 105), the client component will activate the scanner. All the communications with scanner is done through the Vendor supplier drivers and support software.

20 In case of fingerprint security, the user will be directed to place their finger on the scanner and in other cases, the user will be directed to follow the steps provided based on the type of "biometrics" technology used.

25 When the "biometrics" data is successfully obtained from the user (step 106), then the client component will identify the unique physical or behavioral characteristics (step 107) and will convert them into a binary data.

The client component will use the standard encryption method and compression (step 108) and then the processed data will be sent to the invention's server component at the server.

30 The server component will validate the data and will store the "biometrics" data in the database server (step 109).

After step 109, the process is completed the server component will redirect the web-web-browser to the web-page as required by the web-site.

From the steps 103 to 109 the connection between the server and the client component will be open. Any disconnection either by the client component or the server component will be taken as the termination of the process and the finalization procedures will be run for the processes in the server and the client. This includes clearing of buffers, temporary areas, swap areas and other operations as required.

The finalization procedure herein mentioned will also be executed during the successful completion of the process as illustrated in FIGURE 1.

Figure 2, is a flow diagram of the process for online enrollment of "biometrics" data for an existing user in a web-site. The process explained in the diagram is for storing the "biometrics" data, that will be used for verification during the authentication on a web-site. The enrollment process is a standard process but may vary depending upon the requirements of the web-site. The "biometrics" data will be stored in the database server for an user identified by the unique identity in the web-site or in the real world. The database server will reside along with the web-site so as to maintain the consistency of the data for other web-sites stored on the same server.

The process initiator is the client software component which is installed and used in step 206. Before the step 206 as in the step 201, the user enters the required information and the entered information is validated for the existence of the user in the web-site (step 202). The information required by the web-site are designed and implemented in the web-site by the administrator of the web-site and the web-site will call the invention's authentication program for activating the core process of enrollment.

The basic requirement for the invention to select the "biometrics" data, is the unique identifier which is also used during verification/authentication of "biometrics" data. This unique identifier that is generated by the web-site or entered by the user will be sent to the invention's authentication module. The authentication module will then redirect the web-browser to the enrollment page and the step 206 start to process the data given.

The identifier is unique throughout the user database of the invention's database server. The client components introduced in step 206 of this process, will be in form of a downloadable components (like ActiveX, Plug-in, Java Applets) that will be compatible with all the available web-browsers which is the main user-interface for the user. The versions of the component will be maintained so that the Web-Browser will automatically download the latest components.

The invention's authentication module at the server will check for the existence of any stored "biometrics" information for the user,(if any). An informative message will be displayed (step 205) and the process will be terminated.

5 The execution of the step 206, is wholly taken care by the web-browser and the deployment of the components is made compatible for the same. In the step 206, all the drivers and other necessary software components will be downloaded to the client PC.

At step 207, the client component will start processing the data. Firstly, it will check for existing of the "Biometrics" scanner. This is done by communicating with the "Biometrics" scanner specified protocol and the "Biometrics" Scanner vendor supplied drivers.

10 If the "Biometrics" scanner is not present or connected and if any problem in communicating with the "Biometrics" scanner by the client component, the client component will immediately display the informative message 208 related to the cause of the communication problem.

15 The client component will also guide the user with the troubleshooting steps (if any) to rectify the communication problem. If the problem persists, the client component will immediately terminate the process by disconnecting itself from the server component. When server component, is disconnected from the client component it will terminate the process at the server and will redirect the web-browser to a web-page, from where the user will be guided.

20 However, if the "Biometrics" scanner is present and connected the client component will activate the scanner (step 209). All the communications with scanner is done through the Vendor supplier drivers and support softwares.

In case of fingerprint security, the user will be directed to place their finger on the scanner and in another case, the user will be directed to follow the steps provided for based on the type of "biometrics" technology used.

25 When the "biometrics" data is successfully obtained from the user (step 210), then the client component will identify the unique physical or behavioral characteristics (step 211) and will convert them into a binary data.

The client component will use the standard encryption method and compression (step 212), and the processed data will be sent to the invention's server component at the server.

30 The server component will validate the data sent and will store the "biometrics" data in the database server (step 213). The server component will store the "biometrics" data based on

the unique identifier sent to the server's authentication module by the application at the web-site

After step 213, the process is completed and the server component will redirect the web-web-browser to the web-page as required by the web-site.

5 From the steps 206 to 213 the connection between the server and the client component will be open. Any disconnection either by the client component or the server component will be taken as the termination of the process and the finalization procedures will be run for the processes in the server and the client. This includes clearing of buffers, temporary areas, swap areas and other operations as required.

10 The finalization procedure herein mentioned will also be executed during the successful completion of the process as illustrated in FIGURE 2.

Figure 3, is a flow diagram of the process for online enrollment of additional "biometrics" data for an existing enrolled user in a web-site. The process explained in the diagram is for storing the "biometrics" data, that will be also used for verification during the authentication on a web-site. In the process of fingerprint verification, this additional fingerprint storage will help in reducing the false rejection during verification and facilitates the user to use any of the enrolled fingers during verification.

The enrollment process is standard process but it may vary depending upon the requirements of the web-site. The "biometrics" data will be stored in the database server for an user identified by the unique identity in the web-site or in the real world. The database server will reside along with the web-site so as to maintain the consistency of the data for other web-sites stored on the same server.

20 The process initiator is the client software component which is installed and used in the step 307. Before the step 307, in the step 301, the user enters the required information and the information entered is validated for the existence of the user in the web-site (step 302). The information required by the web-site are designed and will be implemented in the web-site by the administrator of the web-site and the web-site will call the invention's authentication program for activating the core process of enrollment.

25 The invention's authentication program will check for the existence of stored "biometrics" data. If no data is stored, then the process will be terminated with an informative message (step 304). This is done mainly to redirect the user to use the process as illustrated in FIGURE 1. This checking for termination of the process, in case of the new user is optional.

Upon verification, the unique identifier is selected from the user's database and sent to the server authentication module. The unique identifier is the basic requirement for the invention to select the "biometrics" data and is also used for verification/authentication. The authentication module will redirect the web-browser to the enrollment page from where step 307 starts processing.

The identifier is unique throughout the user database of the invention's database server. The client components introduced in step 307 of this process, will be in a downloadable components (like ActiveX, Plug-in, Java Applets) that will be compatible with all the available web-browsers which is the main user-interface for the user. The versions of the component will be maintained so that the Web-Browser will automatically download the latest components.

The execution of the step 307, is wholly taken care by the web-browser and the deployment of the components is made compatible for the same. In step 307, all the drivers and other necessary software components will be downloaded to the client PC.

From step 308, the client component will start processing the data. Firstly, it will check for existing "Biometrics" scanner (step 308). This is done by communicating with the "Biometrics" scanner specified protocol by using the "Biometrics" Scanner vendor supplied drivers.

If the "Biometrics" scanner is not present or there is no connection or if there is any problem in communicating with the "Biometrics" scanner by the client component, the client component will immediately display an informative message 309 related to the cause of the communication problem.

The client component will also guide the user with the troubleshooting steps (if any) to rectify the communication problem. If the problem persists, the client component will immediately terminate the process by disconnecting itself from the server component. When the server component is disconnected from the client component it will terminate the process at the server and will redirect the web-browser to a web-page, from where the user will be guided.

However, if the "Biometrics" scanner is present (310), the client component will activate the scanner. All the communications with scanner is done through the Vendor supplier drivers and support softwares.

In case of fingerprint security, the user will be directed to place their finger on the scanner and in another case, the user will be directed to follow the steps provided based on the type of "biometrics" technology used.

When the "biometrics" data is successfully obtained from the user in step 311, then the client component will identify the unique physical or behavioral characteristics (step 312) and will convert them into a binary data.

5 The client component will use the standard encryption method and compression (step 313), then the processed data will be sent to the invention's server component at the server.

The server component will validate the data sent and will compare the sent "biometrics" data with the stored biometrics in the database. The identification of the "biometrics" data in the database is done based on the unique identifier sent initially. If the comparison was not successful the process will be terminated with an informative message.

10 If the comparison was successful, the process of enrolling the additional "biometrics" information starts. The process includes activating the scanner (step 315), retrieving the "biometrics" data from the scanner (step 316), creating data from the characteristics (step 317), encrypting and compressing (step 318).

15 After the (step 318), the data is sent to the server. The server will validate the data sent and will store the "biometrics" data sent as additional "biometrics" data that will be used during verification.

20 From the steps 307 to 319 the connection between the server and the client component will be open. Any disconnection either by the client component or the server component will be taken as the termination of the process and the finalization procedures will be run for the processes in the server and the client. These include clearing of buffers, temporary areas, swap area and other operations as required.

The finalization procedure herein mentioned will also be executed during the successful completion of the process illustrated in FIGURE 3.

25 Figure 4, is a flow diagram of the process for online verification of stored "biometrics" data for an existing enrolled user in a web-site.

30 The enrollment process is standard but may vary depending upon the requirements of the web-site. The "biometrics" data will be stored in the database server for an user identified by the unique identity in the web-site or in the real world. The database server will reside along with the web-site so as to maintain the consistency of the data for other web-sites stored on the same server.

The process initiator is the client software component which is installed and used in the step 404. Before the step 404, in the step 401, the user enters the required information and the

information entered is validated for the existence of the user in the web-site. The information required by the web-site are designed and will be implemented in the web-site by the administrator of the web-site and the web-site will call the invention's authentication program for activating the core process of enrollment.

5 The invention's authentication program will check for the existence of stored "biometrics" data (step 402). If no data was stored, then the process will be terminated with an informative message (step 403).

 Upon verification, the unique identifier is selected from the user's database and sent to the server authentication module. The unique identifier is the basic requirement for the invention to select the "biometrics" data and is also used for verification/authentication. The authentication module will redirect the web-browser to the enrollment page from where the step 404 processing starts.

10 The identifier is unique throughout the user database of the invention's database server. The client components introduced in step 404 of this process, will be in form of downloadable components (like ActiveX, Plug-in, Java Applets) that will be compatible with all the available web-browsers which is the main user-interface for the user. The versioning of the component will be maintained so that the Web-Browser will automatically download the latest components.

 The execution of the step 404, is wholly taken care by the web-browser and the deployment of the components is made compatible for the same. In the step 404, all the drivers and other necessary software components will be downloaded to the client PC.

20 From step 405, the client component will start processing. The first will be the checking for existence of the "Biometrics" scanner (step 405). This is done by communicating using the the "Biometrics" scanner specified protocol using the "Biometrics" Scanner vendor supplied drivers.

25 If the "Biometrics" scanner was not present or connection or if any problem in communicating with the "Biometrics" scanner by the client component, the client component will immediately display an informative message 406 related to the cause of the communication problem.

30 The client component will also guide the user with the troubleshooting steps (if any) to rectify the communication problem. In case if the problem persists, the client component will immediately terminate the process by disconnecting itself from the server component. The

server component, upon disconnection by the client component will terminate the process at the server and will redirect the web-browser to a web-page, from where the user will be guided.

If the "Biometrics" scanner was present, the client component will activate the scanner (step 407). All the communications with scanner is done through the Vendor supplier drivers and support software.

In case of fingerprint security, the user will be directed to place the finger on the scanner and in other cases, the user will be directed to follow the steps provided based on the type of "biometrics" technology used.

When the "biometrics" data is successfully obtained from the user in the step 408, then the client component will identify the unique physical or behavioral characteristics (step 409) and will convert them into a binary data.

The client component will use the standard encryption method and compression (step 410), then the processed data will be sent to the invention's server component at the server.

The server component will validate the data sent and will compare the sent "biometrics" data with the one stored in the database (step 411). The identification of the "biometrics" data in the database is done based on the unique identifier sent initially. If the comparison was not successful the process will be terminated with an informative message (step 412). The error status will be returned to the application in the web-site for further actions.

If the comparison was successful, the success status will be returned to the application in the web-site for further actions. From the steps 405 to 411 the connection between the server and the client component will be open. Any disconnection either by the client component or the server component will be taken as the termination of the process and the finalization procedures will be run for the processes in the server and the client. These include clearing of buffers, temporary areas, swap area and other operations as required.

The finalization procedure herein mentioned will also be executed during the successful completion of the process illustrated in FIGURE 4.

Figure 5, is a flow diagram of the process for online enrollment of "biometrics" data for Credit Card users.

The enrollment process is standard but may vary depending upon the requirements of the web-site. The "biometrics" data will be stored in the database server for an user identified by the unique identity in the web-site or in the real world. The database server will reside along

with the web-site so as to maintain the consistency of the data for other web-sites stored on the same server.

5 The process initiator is the client software component which is installed and used in the step 504. Before the step 504, in the step 501, the user enters the credit card information and the entered information is validated with the credit card database. The credit card information may vary depending upon the requirement of the web-site or type of credit card. If the information is not valid, the process will be terminated by displaying an informative message (step 503).

10 If the information is valid, the Credit Card # or any other unique identifier (generated or entered by the user) will be sent to the invention's authentication program, for activating the core process of enrollment.

 The invention's authentication program will check for the existence of stored "biometrics" data. If any "biometrics" data exists, then the process will be terminated with an informative message.

15 The identifier is unique throughout the user database of the invention's database server. The client components introduced in step 504 of this process, will be in form of downloadable components (like ActiveX, Plug-in, Java Applets) that will be compatible with all the available web-browsers which is the main user-interface for the user. The versioning of the component will be maintained so that the Web-Browser will automatically download the latest components.

20 The execution of the step 504, is wholly taken care by the web-browser and the deployment of the components is made compatible for the same. In the step 504, all the drivers and other necessary software components will be downloaded to the client PC.

25 From step 505, the client component will start processing. The first will be the checking for existence of the "Biometrics" scanner (step 505). This is done by communicating using the the "Biometrics" scanner specified protocol using the "Biometrics" Scanner vendor supplied drivers.

30 If the "Biometrics" scanner was not present or connection or if any problem in communicating with the "Biometrics" scanner by the client component, the client component will immediately display an informative message 506 related to the cause of the communication problem.

The client component will also guide the user with the troubleshooting steps (if any) to rectify the communication problem. In case if the problem persists, the client component will immediately terminate the process by disconnecting itself from the server component. The server component, upon disconnection by the client component will terminate the process at the server and will redirect the web-browser to a web-page, from where the user will be guided.

If the "Biometrics" scanner was present , the client component will activate the scanner (step 507). All the communications with scanner is done through the Vendor supplier drivers and support software.

In case of fingerprint security, the user will be directed to place the finger on the scanner and in other cases, the user will be directed to follow the steps provided based on the type of "biometrics" technology used.

When the "biometrics" data is successfully obtained from the user in the step 508, then the client component will identify the unique physical or behavioral characteristics (step 509) and will convert them into a binary data.

The client component will use the standard encryption method and compression (step 510), then the processed data will be sent to the invention's server component at the server.

The server component will validate the data sent and will store the "biometrics" data sent in the database based on the unique identifier sent by the web-site application. From the steps 504 to 511 the connection between the server and the client component will be open. Any disconnection either by the client component or the server component will be taken as the termination of the process and the finalization procedures will be run for the processes in the server and the client. These include clearing of buffers, temporary areas, swap area and other operations as required.

The finalization procedure herein mentioned will also be executed during the successful completion of the process illustrated in FIGURE 5.

Figure 6, is a flow diagram of the process for online authentication using biometrics in an electronic commerce transaction for credit card users.

For this process, the "biometrics" data of the credit card users must be enrolled using the process illustrated in Figure 1 and 3.

This process is only the authentication process that validates the user and the actual electronic commerce application is not illustrated here. This process may occur before or after the electronic commerce process, based on the application design.

The basic requirement for this authentication process, is the unique identifier that is generated or entered by the user. In the case, the user enters, the Credit card number may be used as identifier and the "biometrics" data will be stored based on identifier, so that during verification the "biometrics" data is selected using the identifier.

5 In this process, in the step 601, user enters the Credit Card details as required by the web-site or other authentication authorities for Credit Card.

The entered information will be validated by the web-site or Credit Card authentication authorities and if the entered information is not valid, the process will be terminated immediately by displaying the message. This process is implemented by the web-site and the
10 invention's role does not interfere yet.

The authentication process by the invention's program starts from the step 602, after the credit card details provided by the user is valid. The invention's authentication program at the server, is activated by providing the unique identifier that will be used for verification.

The process initiator for the invention's authentication program is the client software
15 component which is installed and used in the step 604.

The invention's authentication program will check for the existence of stored "biometrics" data (step 602). If no data was stored for the unique identifier, then the process will be terminated with an informative message (step 603).

The client components introduced in step 604 of this process, will be in form of
20 downloadable components (like ActiveX, Plug-in, Java Applets) that will be compatible with all the available web-browsers which is the main user-interface for the user. The versioning of the component will be maintained so that the Web-Browser will automatically download the latest components.

The execution of the step 604, is wholly taken care by the web-browser and the
25 deployment of the components is made compatible for the same. In the step 604, all the drivers and other necessary software components will be downloaded to the client PC.

From step 605, the client component will start processing. The first will be the checking for existence of the "Biometrics" scanner (step 605). This is done by communicating using the the "Biometrics" scanner specified protocol using the "Biometrics" Scanner vendor supplied
30 drivers.

If the "Biometrics" scanner was not present or connection or if any problem in communicating with the "Biometrics" scanner by the client component, the client component

will immediately display an informative message 606 related to the cause of the communication problem.

The client component will also guide the user with the troubleshooting steps (if any) to rectify the communication problem. In case if the problem persists, the client component will immediately terminate the process by disconnecting itself from the server component. The server component, upon disconnection by the client component will terminate the process at the server and will redirect the web-browser to a web-page, from where the user will be guided.

If the "Biometrics" scanner was present , the client component will activate the scanner (step 607). All the communications with scanner is done through the Vendor supplier drivers and support software.

In case of fingerprint security, the user will be directed to place the finger on the scanner and in other cases, the user will be directed to follow the steps provided based on the type of "biometrics" technology used.

When the "biometrics" data is successfully obtained from the user in the step 608, then the client component will identify the unique physical or behavioral characteristics (step 609) and will convert them into a binary data.

The client component will use the standard encryption method and compression (step 610), then the processed data will be sent to the invention's server component at the server.

The server component will validate the data sent and will compare the sent "biometrics" data with the one stored in the database (step 611). The identification of the "biometrics" data in the database is done based on the unique identifier sent initially. If the comparison was not successful the process will be terminated with an informative message (step 612). The error status will be returned to the application in the web-site for further actions.

If the comparison was successful, the success status will be returned to the application in the web-site for further actions. From the steps 605 to 611 the connection between the server and the client component will be open. Any disconnection either by the client component or the server component will be taken as the termination of the process and the finalization procedures will be run for the processes in the server and the client. These include clearing of buffers, temporary areas, swap area and other operations as required.

The finalization procedure herein mentioned will also be executed during the successful completion of the process illustrated in FIGURE 6.

Figure 7, is a flow diagram of the process for online authentication using biometrics in an electronic commerce transaction for other identification methods.

For this process, the "biometrics" data of the users must be enrolled using the process illustrated in Figure 1 and 3.

5 This process is only the authentication process that validates the user and the actual electronic commerce application is not illustrated here. This process may occur before or after the electronic commerce process, based on the application design.

10 The basic requirement for this authentication process, is the unique identifier that is generated or entered by the user. In the case, the user enters, the User Name/ID for example, that may be used as identifier and the "biometrics" data will be stored based on identifier, so that during verification the "biometrics" data is also selected using the identifier.

In this process, in the step 701, user enters the identification details as required by the web-site.

15 The entered information will be validated by the web-site and if the entered information is not valid, the process will be terminated immediately by displaying the message. This process is implemented by the web-site and the invention's role does not interfere yet.

The authentication process by the invention's program starts from the step 702, after the identification details provided by the user is valid. The invention's authentication program at the server, is activated by providing the unique identifier that will be used for verification.

20 The process initiator for the invention's authentication program is the client software component which is installed and used in the step 704.

The invention's authentication program will check for the existence of stored "biometrics" data (step 702). If no data was stored for the unique identifier, then the process will be terminated with an informative message (step 703).

25 The client components introduced in step 704 of this process, will be in form of downloadable components (like ActiveX, Plug-in, Java Applets) that will be compatible with all the available web-browsers which is the main user-interface for the user. The versioning of the component will be maintained so that the Web-Browser will automatically download the latest components.

30 The execution of the step 704, is wholly taken care by the web-browser and the deployment of the components is made compatible for the same. In the step 704, all the drivers and other necessary software components will be downloaded to the client PC.

From step 705, the client component will start processing. The first will be the checking for existence of the "Biometrics" scanner (step 705). This is done by communicating using the the "Biometrics" scanner specified protocol using the "Biometrics" Scanner vendor supplied drivers.

5 If the "Biometrics" scanner was not present or connection or if any problem in communicating with the "Biometrics" scanner by the client component, the client component will immediately display an informative message 706 related to the cause of the communication problem.

10 The client component will also guide the user with the troubleshooting steps (if any) to rectify the communication problem. In case if the problem persists, the client component will immediately terminate the process by disconnecting itself from the server component. The server component, upon disconnection by the client component will terminate the process at the server and will redirect the web-browser to a web-page, from where the user will be guided.

15 If the "Biometrics" scanner was present , the client component will activate the scanner (step 707). All the communications with scanner is done through the Vendor supplier drivers and support software.

In case of fingerprint security, the user will be directed to place the finger on the scanner and in other cases, the user will be directed to follow the steps provided based on the type of "biometrics" technology used.

20 When the "biometrics" data is successfully obtained from the user in the step 708, then the client component will identify the unique physical or behavioral characteristics (step 709) and will convert them into a binary data.

The client component will use the standard encryption method and compression (step 710), then the processed data will be sent to the invention's server component at the server.

25 The server component will validate the data sent and will compare the sent "biometrics" data with the one stored in the database (step 711). The identification of the "biometrics" data in the database is done based on the unique identifier sent initially. If the comparison was not successful the process will be terminated with an informative message (step 712). The error status will be returned to the application in the web-site for further actions.

30 If the comparison was successful, the success status will be returned to the application in the web-site for further actions. From the steps 705 to 711 the connection between the server and the client component will be open. Any disconnection either by the client

component or the server component will be taken as the termination of the process and the finalization procedures will be run for the processes in the server and the client. These include clearing of buffers, temporary areas, swap area and other operations as required.

5 The finalization procedure herein mentioned will also be executed during the successful completion of the process illustrated in FIGURE 7.

Figure 8, is a flow diagram of the process for online authentication using biometrics in an ATM transaction. The process with is a part of the invention may be used by the financial institution or any other entity which uses ATM to serve its customers.

10 For this process, the "biometrics" data of the users must be enrolled using the process illustrated in Figure 1 and 3 with the ATM card number as the unique identifier (optional).

This process is only the authentication process that validates the user and the actual ATM application is not illustrated here. This process may occur before or after the ATM transaction, based on the application design.

15 The basic requirement for this authentication process, is the unique identifier that is generated or entered by the user. In an ATM transaction, the unique identifier can be the ATM card number or any other unique identifier and the "biometrics" data will be stored based on identifier, so that during verification the "biometrics" data is also selected using the identifier.

In this process, in the step 801, user inserts the ATM card and enters the PIN as required by the customer.

20 The entered information will be validated and if the entered information is not valid, the process will be terminated immediately by displaying the message. This process is may be implemented earlier and the invention's role does not interfere yet.

25 The authentication process by the invention's program starts from the step 802, after the identification details is provided by the user is valid. The invention's authentication program at the server, is activated by providing the unique identifier that will be used for verification.

The process initiator for the invention's authentication program is the client software component which is installed and used in the step 804.

30 The invention's authentication program will check for the existence of stored "biometrics" data (step 802). If no data was stored for the unique identifier, then the process will be terminated with an informative message (step 803).

The client components introduced in step 804 of this process, will be in form of downloadable components that is automatically downloaded to the client (ATM) if the

component does not exist or is outdated. In the step 804, all the drivers and other necessary software components will be downloaded to the client.

5 From step 805, the client component will start processing. The first will be the checking for existence of the "Biometrics" scanner (step 805). This is done by communicating using the the "Biometrics" scanner specified protocol using the "Biometrics" Scanner vendor supplied drivers.

10 If the "Biometrics" scanner was not present or connection or if any problem in communicating with the "Biometrics" scanner by the client component, the client component will immediately display an informative message 806 related to the cause of the communication problem.

The client component will also guide the user with the troubleshooting steps (if any) to rectify the communication problem. In case if the problem persists, the client component will immediately terminate the process by disconnecting itself from the server component. The server component, upon disconnection by the client component will terminate the process at the server and will redirect the web-browser to a web-page, from where the user will be guided.

15 If the "Biometrics" scanner was present, the client component will activate the scanner (step 807). All the communications with scanner is done through the Vendor supplier drivers and support software.

20 In case of fingerprint security, the user will be directed to place the finger on the scanner and in other cases, the user will be directed to follow the steps provided based on the type of "biometrics" technology used.

When the "biometrics" data is successfully obtained from the user in the step 808, then the client component will identify the unique physical or behavioral characteristics (step 809) and will convert them into a binary data.

25 The client component will use the standard encryption method and compression (step 810), then the processed data will be sent to the invention's server component at the server.

30 The server component will validate the data sent and will compare the sent "biometrics" data with the one stored in the database (step 811). The identification of the "biometrics" data in the database is done based on the unique identifier sent initially. If the comparison was not successful the process will be terminated with an informative message (step 712). The error status will be returned to the application that called the invention's authentication program.

If the comparison was successful, the success status will be returned to the application that called the invention's authentication program for further actions. From the steps 805 to 811 the connection between the server and the client component will be open. Any disconnection either by the client component or the server component will be taken as the termination of the process and the finalization procedures will be run for the processes in the server and the client. These include clearing of buffers, temporary areas, swap area and other operations as required.

The finalization procedure herein mentioned will also be executed during the successful completion of the process illustrated in FIGURE 8.

Figure 9, is a flow diagram of the process for online authentication using biometrics and using invention's authentication server. The invention's authentication server will be connected to the Internet and the web-site (herein called as "Third-party Web-Site") intended to implement the invention's authentication process will link their authentication process to the invention's authentication server. The connectivity between the Third-party Web-site and the invention's authentication server may be through the open network like Internet or Local Area network also called as LAN.

For this process, the "biometrics" data of the users must be enrolled using the process illustrated in Figure 1 and 3 using the unique identifier generated and sent by the application at the third-party web-site.

This process is only the authentication process that validates the user and the actual application is not illustrated here and it is executed on the third-party web-site. The application in the third-party web-site may be linked to the invention's authentication based on the requirement.

The basic requirement for this authentication process, is the unique identifier that is generated or entered by the user and the "biometrics" data will be stored based on identifier, so that during verification the "biometrics" data is also selected using the identifier.

In this process, in the step 901, user enters the identification information in the third-party web-site as required.

The entered information will be validated and if the entered information is not valid, the process will be terminated immediately by displaying the message. This process of validating the information entered is implemented only by the third-party web-site

The authentication process by the invention's program starts from the step 802, after the identification details is provided by the user is valid. The invention's authentication program at the server, is activated by providing the unique identifier that will be used for verification. The application in the third-party web-site will be linked to the authentication server by redirecting the web-browser to the authentication page on the authentication server.

The process initiator for the invention's authentication program is the client software component which is installed and used in the step 904.

The invention's authentication program will check for the existence of stored "biometrics" data (step 902). If no data was stored for the unique identifier, then the process will be terminated with an informative message (step 903).

The client components introduced in step 904 of this process, will be in form of downloadable components that is automatically downloaded to the client computer if the component does not exists or if outdated. In the step 904, all the drivers and other necessary software components will be downloaded to the client PC.

From step 8059 the client component will start processing. The first will be the checking for existence of the "Biometrics" scanner (step 905). This is done by communicating using the the "Biometrics" scanner specified protocol using the "Biometrics" Scanner vendor supplied drivers.

If the "Biometrics" scanner was not present or connection or if any problem in communicating with the "Biometrics" scanner by the client component, the client component will immediately display an informative message 906 related to the cause of the communication problem.

The client component will also guide the user with the troubleshooting steps (if any) to rectify the communication problem. In case if the problem persists, the client component will immediately terminate the process by disconnecting itself from the server component. The server component, upon disconnection by the client component will terminate the process at the server and will redirect the web-browser to a web-page, from where the user will be guided.

If the "Biometrics" scanner was present , the client component will activate the scanner (step 907). All the communications with scanner is done through the Vendor supplier drivers and support software.

In case of fingerprint security, the user will be directed to place the finger on the scanner and in other cases, the user will be directed to follow the steps provided based on the type of "biometrics" technology used.

5 When the "biometrics" data is successfully obtained from the user in the step 908, then the client component will identify the unique physical or behavioral characteristics (step 909) and will convert them into a binary data.

The client component will use the standard encryption method and compression (step 910), then the processed data will be sent to the invention's server component at the server.

10 The server component will validate the data sent and will compare the sent "biometrics" data with the one stored in the database (step 911). The identification of the "biometrics" data in the database is done based on the unique identifier sent initially. If the comparison was not successful the process will be terminated with an informative message (step 912). The error status will be returned to the application that called the invention's authentication program.

15 If the comparison was successful, the success status will be returned to the application that called the invention's authentication program for further actions. From the steps 905 to 911 the connection between the server and the client component will be open. Any disconnection either by the client component or the server component will be taken as the termination of the process and the finalization procedures will be run for the processes in the server and the client. These include clearing of buffers, temporary areas, swap area and other operations as required.

20 The finalization procedure herein mentioned will also be executed during the successful completion of the process illustrated in FIGURE 9.

25 Figure 10, is a flow diagram of the process for online authentication using biometrics in an internet banking transaction.

For this process, the "biometrics" data of the users must be enrolled using the process illustrated in Figure 1 and 3 based on the bank's unique identifier provided to their customer.

The web-site herein called, is the bank's web-site that facilitates its customer to do banking transaction online, also called as internet banking.

30 This process is only the authentication process that validates the user and the actual internet banking application is not illustrated here. This process may occur before or after the internet banking process, based on the application design.

The basic requirement for this authentication process, is the unique identifier that is generated or entered by the user. In the case, the user enters, the User Name/ID for example, that may be used as identifier and the "biometrics" data will be stored based on identifier, so that during verification the "biometrics" data is also selected using the identifier.

5 In this process, in the step 1001, user enters the identification details as required by the web-site.

The entered information will be validated by the web-site and if the entered information is not valid, the process will be terminated immediately by displaying the message. This process is implemented by the web-site and the invention's role does not interfere yet.

10 The authentication process by the invention's program starts from the step 1002, after the identification details provided by the user is valid. The invention's authentication program at the server, is activated by providing the unique identifier that will be used for verification.

The process initiator for the invention's authentication program is the client software component which is installed and used in the step 1004.

15 The invention's authentication program will check for the existence of stored "biometrics" data (step 1002). If no data was stored for the unique identifier, then the process will be terminated with an informative message (step 1003).

20 The client components introduced in step 1004 of this process, will be in form of downloadable components (like ActiveX, Plug-in, Java Applets) that will be compatible with all the available web-browsers which is the main user-interface for the user. The versioning of the component will be maintained so that the Web-Browser will automatically download the latest components.

25 The execution of the step 1004, is wholly taken care by the web-browser and the deployment of the components is made compatible for the same. In the step 1004, all the drivers and other necessary software components will be downloaded to the client PC.

From step 1005, the client component will start processing. The first will be the checking for existence of the "Biometrics" scanner (step 1005). This is done by communicating using the the "Biometrics" scanner specified protocol using the "Biometrics" Scanner vendor supplied drivers.

30 If the "Biometrics" scanner was not present or connection or if any problem in communicating with the "Biometrics" scanner by the client component, the client component

will immediately display an informative message 1006 related to the cause of the communication problem.

5 The client component will also guide the user with the troubleshooting steps (if any) to rectify the communication problem. In case if the problem persists, the client component will immediately terminate the process by disconnecting itself from the server component. The server component, upon disconnection by the client component will terminate the process at the server and will redirect the web-browser to a web-page, from where the user will be guided.

10 If the "Biometrics" scanner was present , the client component will activate the scanner (step 1007). All the communications with scanner is done through the Vendor supplier drivers and support software.

In case of fingerprint security, the user will be directed to place the finger on the scanner and in other cases, the user will be directed to follow the steps provided based on the type of "biometrics" technology used.

15 When the "biometrics" data is successfully obtained from the user in the step 1008, then the client component will identify the unique physical or behavioral characteristics (step 1009) and will convert them into a binary data.

The client component will use the standard encryption method and compression (step 1010), then the processed data will be sent to the invention's server component at the server.

20 The server component will validate the data sent and will compare the sent "biometrics" data with the one stored in the database (step 1011). The identification of the "biometrics" data in the database is done based on the unique identifier sent initially. If the comparison was not successful the process will be terminated with an informative message (step 1012). The error status will be returned to the application in the web-site for further actions.

25 If the comparison was successful, the success status will be returned to the application in the web-site for further actions. From the steps 1005 to 1011 the connection between the server and the client component will be open. Any disconnection either by the client component or the server component will be taken as the termination of the process and the finalization procedures will be run for the processes in the server and the client. These include clearing of
30 buffers, temporary areas, swap area and other operations as required.

The finalization procedure herein mentioned will also be executed during the successful completion of the process illustrated in FIGURE 10.

Figure 11, is a flow diagram of the process for online authentication in software applications.

For this process, the "biometrics" data of the users must be enrolled using the process illustrated in Figure 1 and 3 based on the unique identifier used for identifying users in the application.

This process is only the authentication process that validates the user and the actual application is not illustrated here. This process may occur before or after the existing authentication process, based on the application design.

The basic requirement for this authentication process, is the unique identifier that is generated or entered by the user. In the case, the user enters, the User Name/ID for example, that may be used as identifier and the "biometrics" data will be stored based on identifier, so that during verification the "biometrics" data is also selected using the identifier.

In this process, in the step 1101, user enters the identification details as required by the application.

The entered information will be validated by the application and if the entered information is not valid, the process will be terminated immediately by displaying the message. This process is implemented by the application and the invention's role does not interfere yet.

The authentication process by the invention's program starts from the step 1102, after the identification details provided by the user is valid. The invention's authentication program at the server, is activated by providing the unique identifier that will be used for verification.

The process initiator for the invention's authentication program is the client software component which is installed and used in the step 1104.

The invention's authentication program will check for the existence of stored "biometrics" data (step 1102). If no data was stored for the unique identifier, then the process will be terminated with an informative message (step 1103).

The client components introduced in step 1104 of this process, will be in form of downloadable components. The versioning of the component will be maintained so that the latest components will be downloaded automatically to the client PC

In the step 1104, all the drivers and other necessary software components will be downloaded to the client PC.

From step 1105, the client component will start processing. The first will be the checking for existence of the "Biometrics" scanner (step 1105). This is done by communicating

using the the "Biometrics" scanner specified protocol using the "Biometrics" Scanner vendor supplied drivers.

5 If the "Biometrics" scanner was not present or connection or if any problem in communicating with the "Biometrics" scanner by the client component, the client component will immediately display an informative message 1106 related to the cause of the communication problem.

10 The client component will also guide the user with the troubleshooting steps (if any) to rectify the communication problem. In case if the problem persists, the client component will immediately terminate the process by disconnecting itself from the server component. The server component, upon disconnection by the client component will terminate the process at the server.

If the "Biometrics" scanner was present , the client component will activate the scanner (step 1107). All the communications with scanner is done through the Vendor supplier drivers and support software.

15 In case of fingerprint security, the user will be directed to place the finger on the scanner and in other cases, the user will be directed to follow the steps provided based on the type of "biometrics" technology used.

20 When the "biometrics" data is successfully obtained from the user in the step 1108, then the client component will identify the unique physical or behavioral characteristics (step 1109) and will convert them into a binary data.

The client component will use the standard encryption method and compression (step 1110), then the processed data will be sent to the invention's server component at the server.

25 The server component will validate the data sent and will compare the sent "biometrics" data with the one stored in the database (step 1111). The identification of the "biometrics" data in the database is done based on the unique identifier sent initially. If the comparison was not successful the process will be terminated with an informative message (step 1112). The error status will be returned to the application for further actions.

30 If the comparison was successful, the success status will be returned to the application for further actions. From the steps 1105 to 1111 the connection between the server and the client component will be open. Any disconnection either by the client component or the server component will be taken as the termination of the process and the finalization procedures will

be run for the processes in the server and the client. These include clearing of buffers, temporary areas, swap area and other operations as required.

The finalization procedure herein mentioned will also be executed during the successful completion of the process illustrated in FIGURE 11.

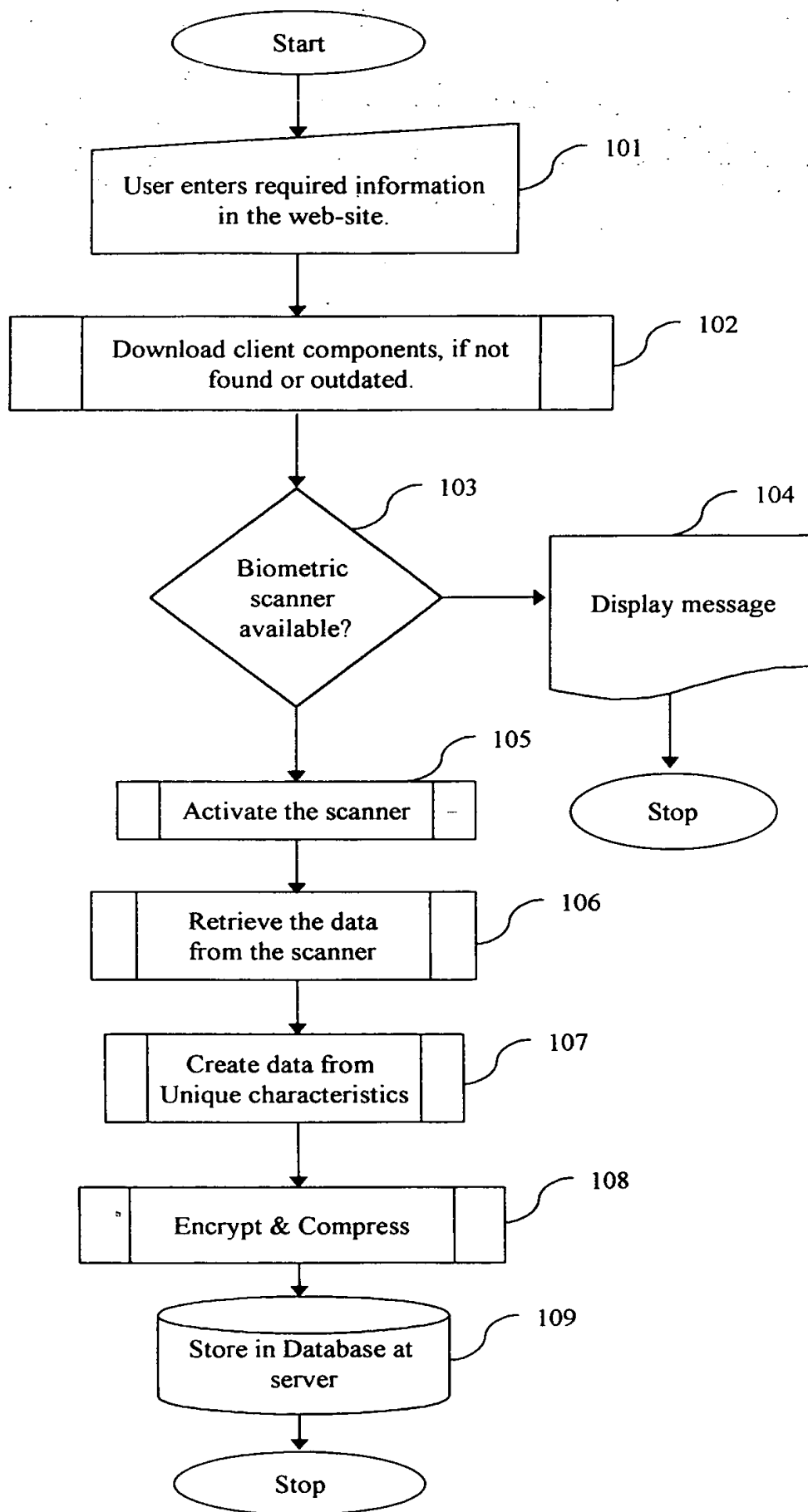
Claims

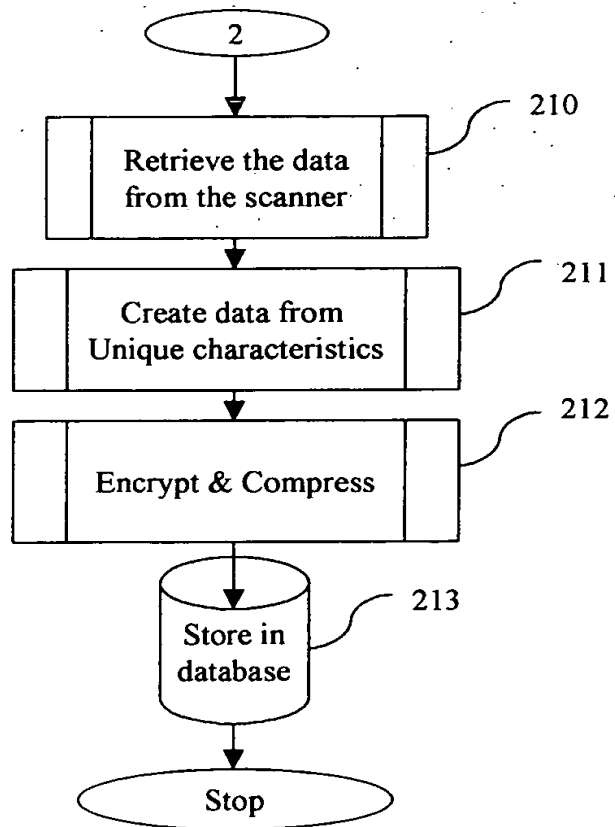
1. A security system for electronic commerce to verify the authenticity of a user comprising: -
 - 5 i) installation of a server authentication program in a web-server at a website of a web-service provider;
 - ii) downloading and installation of client software component at a workstation of the client;
 - 10 iii) integration of the server authentication program with existing web-application with the web-service provider;
 - iv) user entering the existing security parameters;
 - v) activation of biometrics scanner pre-installed at workstation of client gathering biometrics image from biometric scanner, identifying characteristics of biometrics image and converting into digital data;
 - 15 vi) compression and encryption of data from biometric scanner;
 - vii) transmittance of compressed and encrypted data to web-server;
 - viii) — comparison of encrypted data with data stored in database; —
 - ix) sending of status codes of comparison, if comparison is successful, to application at web-service provider.
- 20 2. A security system for electronic commerce to verify the authenticity of a user as claimed in claim 1 wherein the biometrics data is selected from one or more of the following comprising of finger print of one or more fingers, palm print, iris scan and retina scan and any other optically distinguishable parameters of the human body.
- 25 3. A security system for electronic commerce to verify the authenticity of a user as claimed in Claim 1 wherein a plurality of source biometrics data of a single user is used to authenticate the identity of the user.

BIOMETRIC VERIFICATION FOR ELECTRONIC TRANSACTIONS OVER THE WEB**ABSTRACT**

5 A security system for electronic commerce to verify the authenticity of a user
comprising; installation of a server authentication program in a web-server at a website of a
web-service provider; downloading and installation of client software component at a
workstation of the client; integration of the server authentication program with existing web-
application with the web-service provider; user entering the existing security parameters;
10 activation of biometrics scanner pre-installed at workstation of client gathering biometrics image
from biometric scanner, identifying characteristics of biometrics image and converting into
digital data; compression and encryption of data from biometric scanner; transmittance of
compressed and encrypted data to web-server; comparison of encrypted data with data stored
in database; sending of status codes of comparison, if comparison is successful, to application
15 at web-service provider.

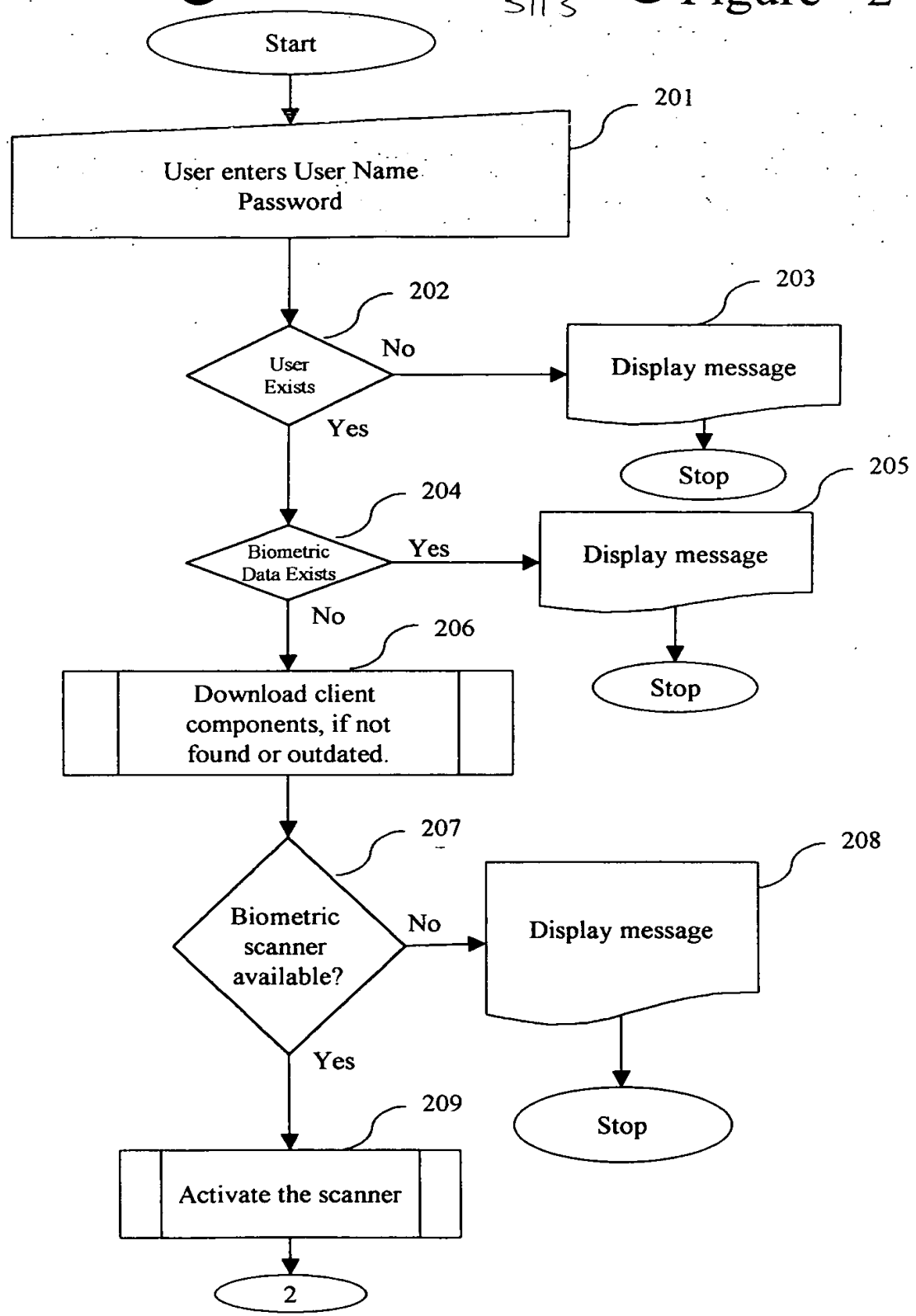
Figure 4



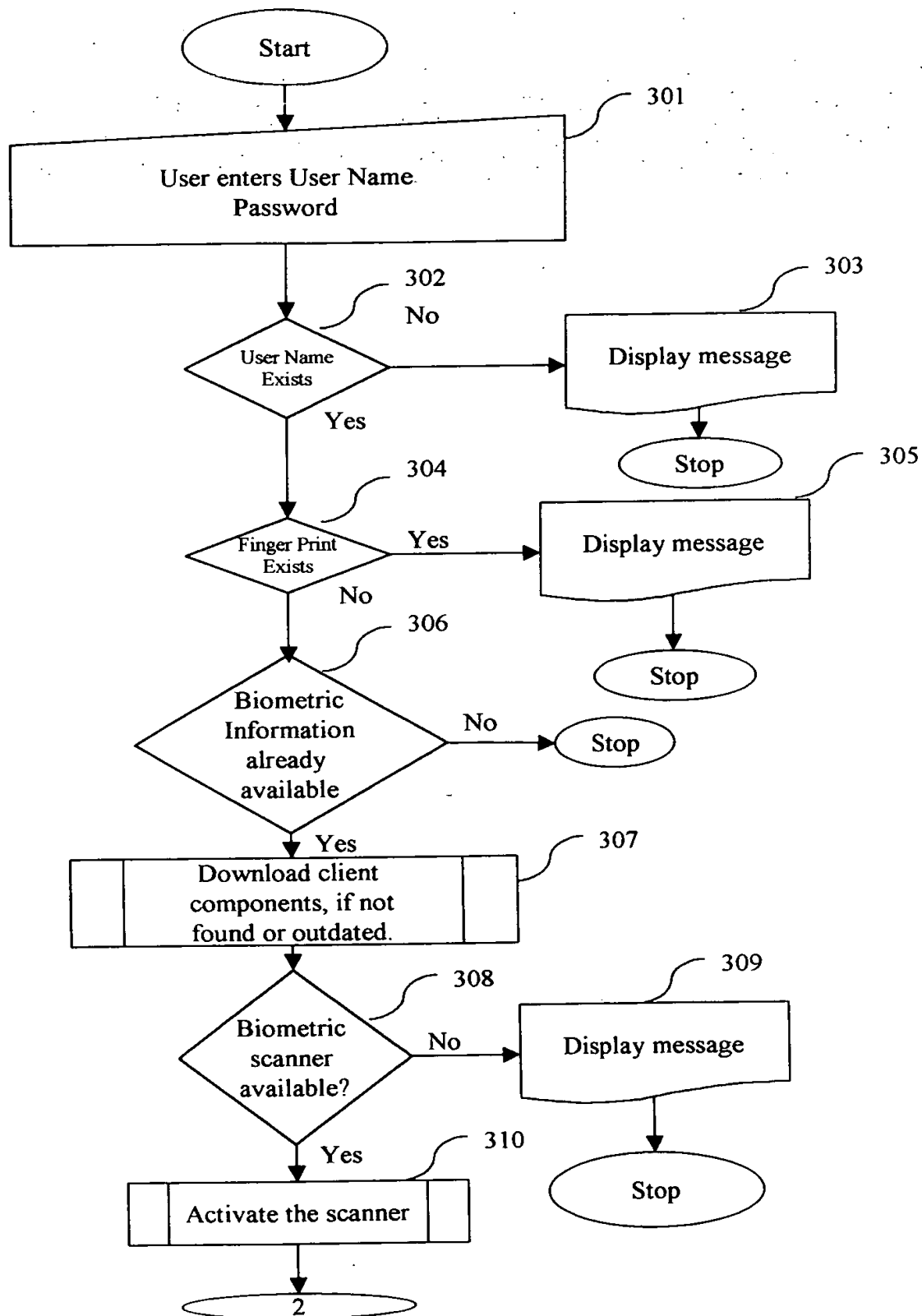


3/13

● Figure - 2



.... continued



... continued

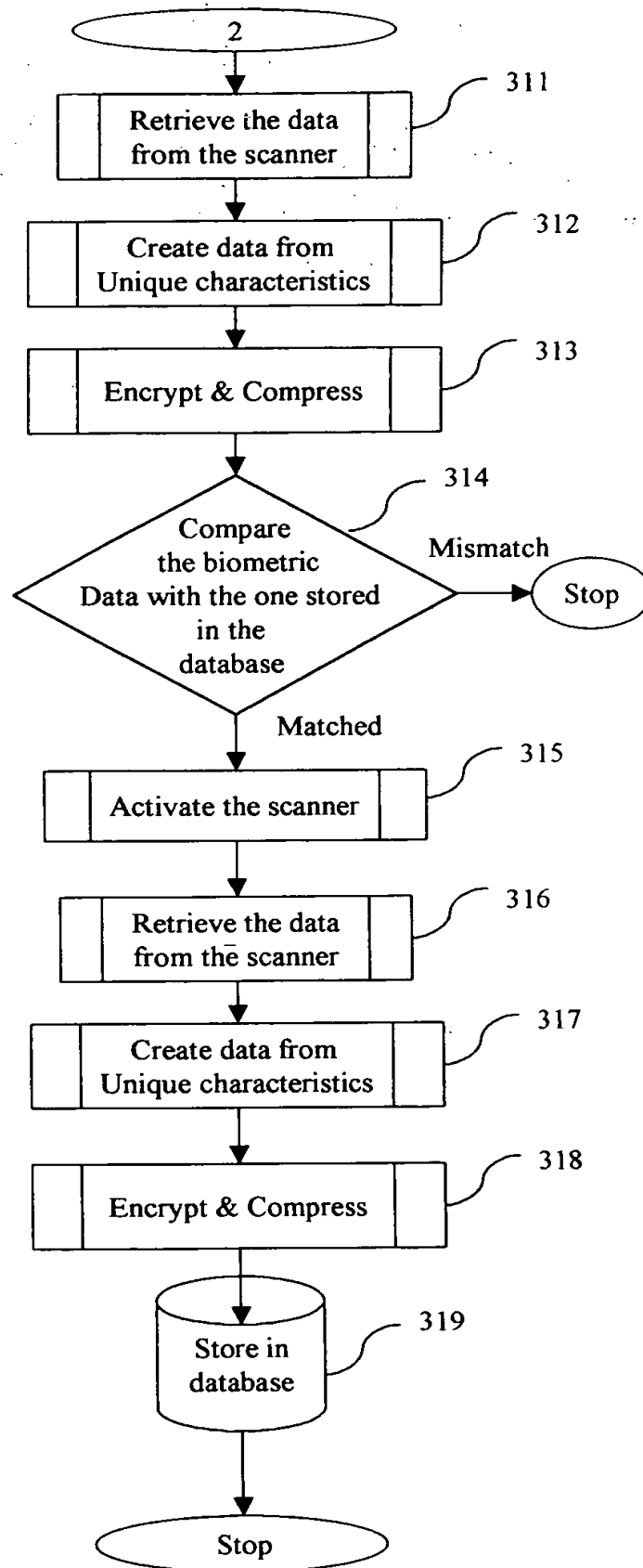
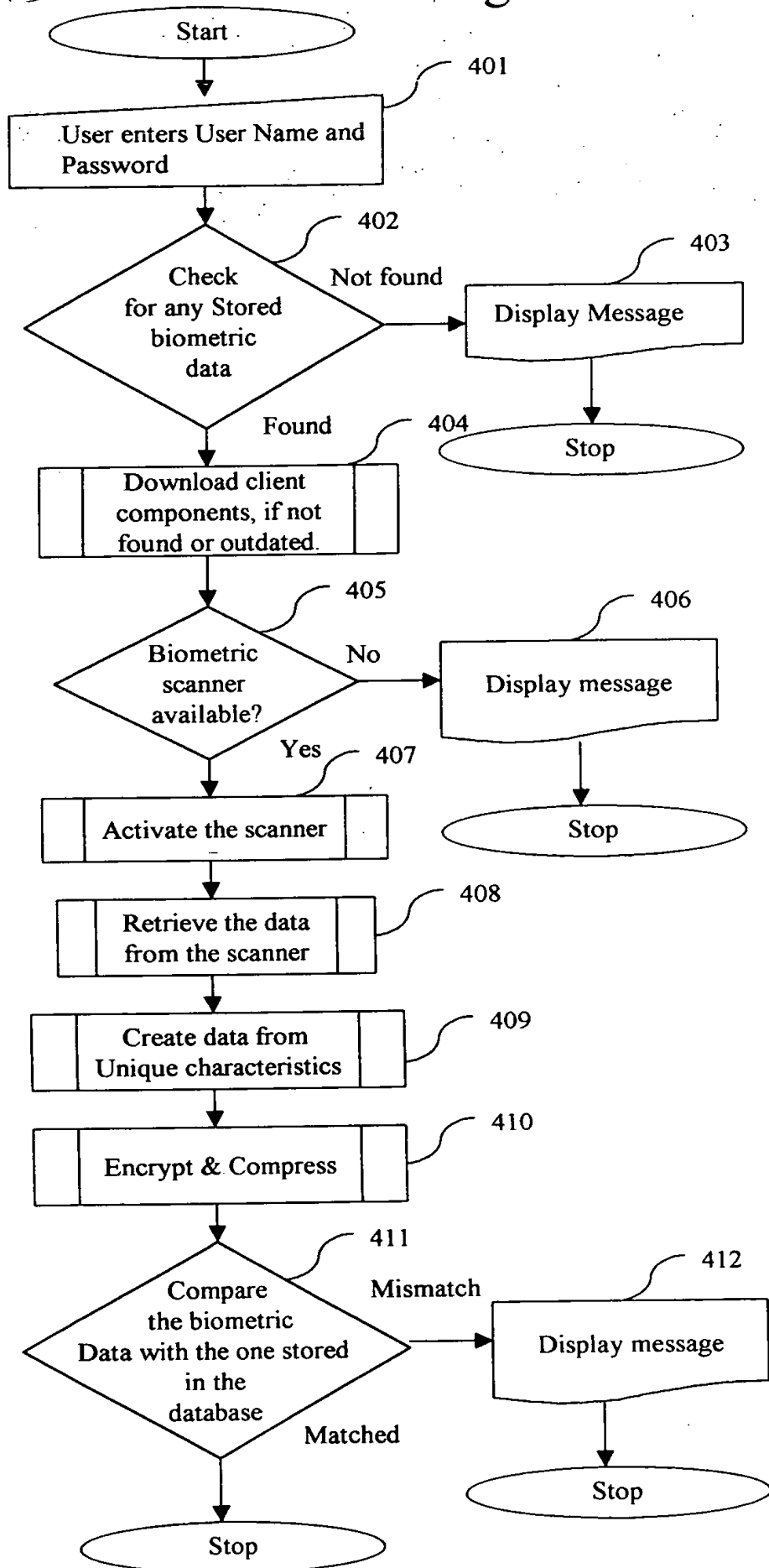
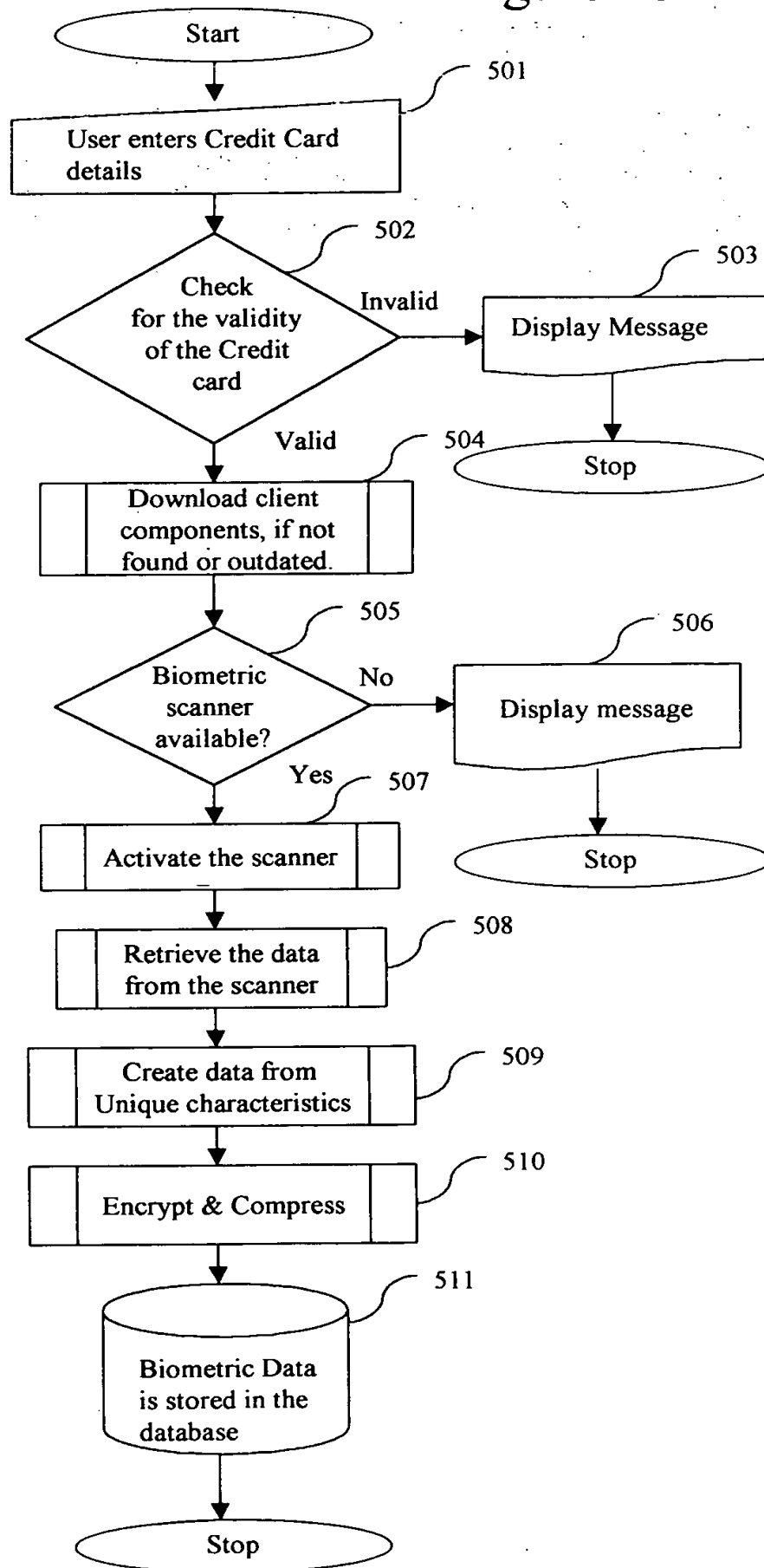
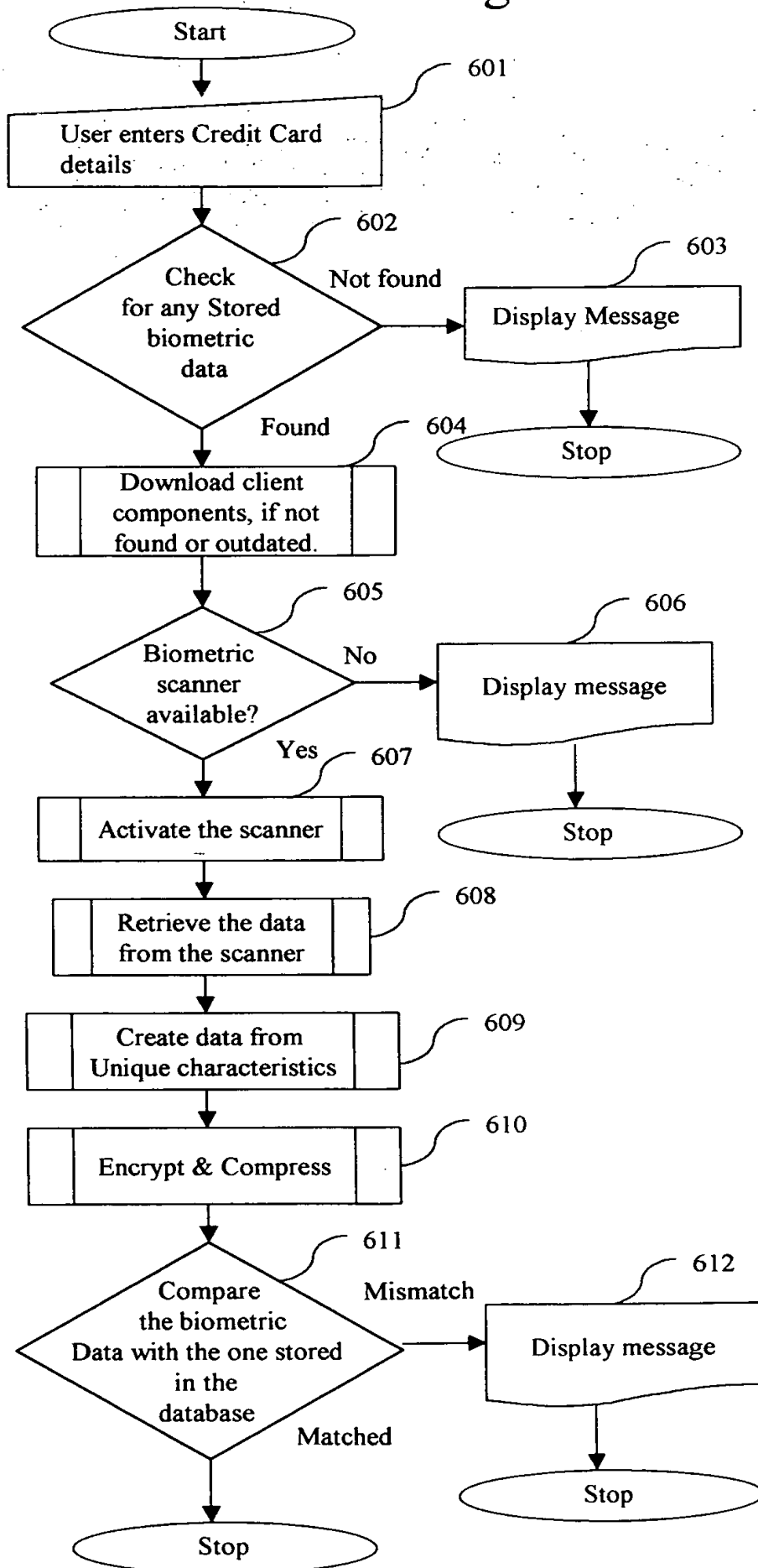
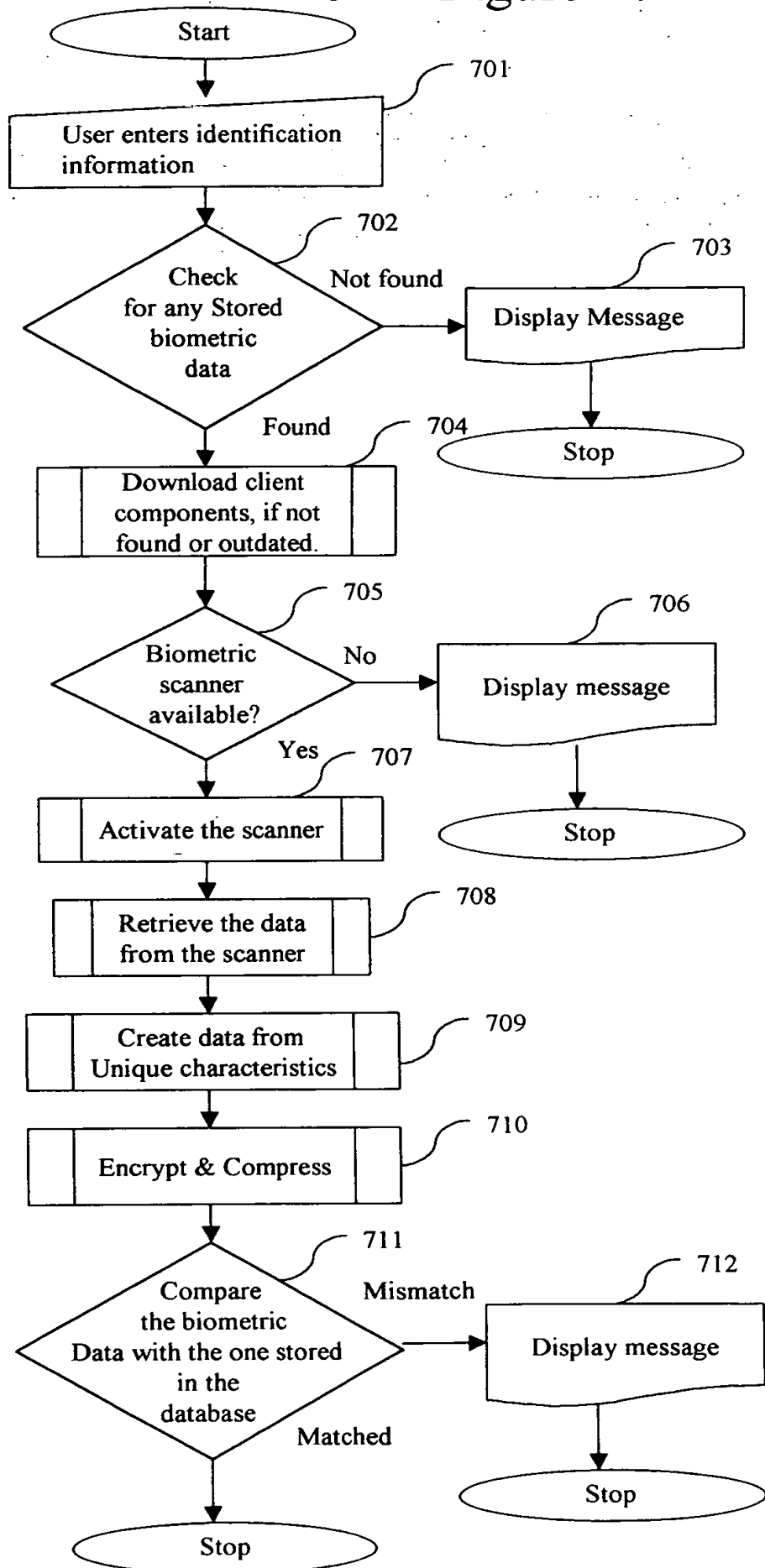


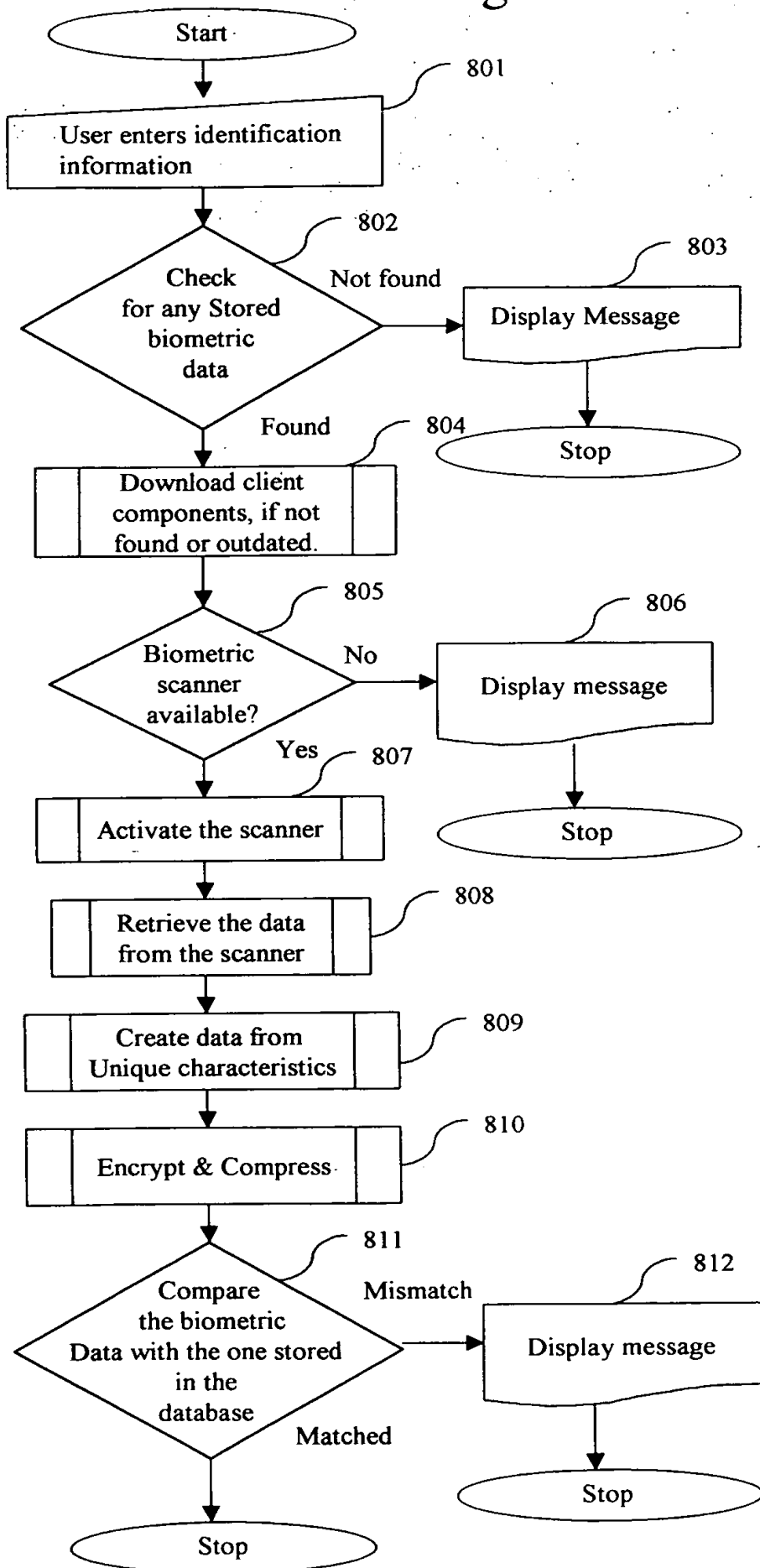
Figure - 4











11/13. Figure - 9

